Journal of Combinatorial Theory, Series A 118 (2011) 1072–1085

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

Unifying some known infinite families of combinatorial 3-designs

Masakazu Jimbo [a], Yuta Kunihara [a], Reinhard Laue [a], Masanori Sawa [b]

[a] *Bayreuth University, Germany*
[b] *Nagoya University, Japan*

A R T I C L E   I N F O

Article history:
Received 9 April 2010
Available online 5 November 2010

Keywords:
Automorphism
Jungnickel–Vanstone method
Köhler theory
Rahilly method
Resolvability
Simplicity
3-Design
Van Tran method

A B S T R A C T

In this paper we present a construction of 3-designs by using a 3-design with resolvability. The basic construction generalizes a well-known construction of simple 3-$(v,4,3)$ designs by Jungnickel and Vanstone (1986). We investigate the conditions under which the designs obtained by the basic construction are simple. Many infinite families of simple 3-designs are presented, which are closely related to some known families by Iwasaki and Meixner (1995), Laue (2004) and van Tran (2000, 2001). On the other hand, the designs obtained by the basic construction possess various properties: A theory of constructing simple cyclic 3-$(v,4,3)$ designs by Köhler (1981) can be readily rebuilt from the context of this paper. Moreover many infinite families of simple resolvable 3-designs are presented in comparison with some known families. We also show that for any prime power q and any odd integer n there exists a resolvable 3-$(q^n+1,q+1,1)$ design. As far as the authors know, this is the first and the only known infinite family of resolvable t-$(v,k,1)$ designs with $t \geqslant 3$ and $k \geqslant 5$. Those resolvable designs can again be used to obtain more infinite families of simple 3-designs through the basic construction.

1. Introduction

Let t, v, k, λ be positive integers such that $v > k > t$. A t-(v,k,λ) *design* is a system of v points V and those k-subsets $\mathcal{B}$, called *blocks*, such that every t-subset of V occurs in exactly λ blocks in $\mathcal{B}$. Values k, λ are respectively called *blocksize* and *index*. A t-design is said to be *simple* if it has no repeated blocks. To construct simple t-designs is one of the most fundamental subjects in

E-mail addresses: laue@uni-bayreuth.de (R. Laue), sawa@is.nagoya-u.ac.jp (M. Sawa).

0097-3165/$ – see front matter
doi:10.1016/j.jcta.2010.10.007

design theory. A well-known theorem of Wilson [42] asymptotically solves the problem for 2-designs. However it is far from settled for t-designs in general even for 3-designs. In this paper we consider the problem for 3-designs.

A classical method of constructing simple 3-designs employs suitable orbits on k-element subsets under the action of the projective general linear (PGL) group or projective special linear (PSL) group on the projective line, with no orbits used repeatedly, and regards them as sets of blocks. The construction generates 3-designs which admit the groups as an automorphism group, whose number of points are a prime power plus one; in some special cases, PGL or PSL can be used to construct simple 3-designs with the number of points being a prime power plus "two" [29,33]. It is not clear when the study of such constructions started, but were already used by Carmichael [14] in 1937 and Witt [43] in 1938. Following their celebrated results, Hughes [21] found several infinite families of simple 3-designs. Since then, many researchers focused on the group-theoretic method and thereby found many simple 3-designs; for example, see [8,13,22].

One of the most common constructions for 3-designs is a recursive method. Hartman [19] developed a recursive technique as an analogue of a standard recursive construction for 2-designs (e.g., see [42]) and thereby found some new infinite families of simple 3-designs. Similar recursive constructions were found by Blanchard [10], Mohácsy and Ray-Chaudhuri [34]. Van Tran [40,41] developed another type of recursive constructions that use a geometric property, called the resolvability, which generalize the well-known doubling construction of 3-$(v,4,1)$ designs, see Carmichael [14] and Witt [43] and some famous constructions of 3-designs with general blocksizes by Driessen [15]. Van Tran's constructions have the merit that they produce designs whose number of points and blocksize are of general form. A similar construction which uses the resolvability was found by Jungnickel and Vanstone [24,25].

The main purpose of this paper is to investigate the existence of simple 3-designs with general parameters. "General parameters" means, in this paper, that they are not necessarily associated with a prime power; whereas, many known families of such designs have parameters which are associated with a prime power [16, pp. 82–83]. This paper is organized as follows. In Section 2 we present a new construction of 3-designs by using the resolvability of a 3-design. The basic construction generalizes a well-known construction of 3-$(v,4,3)$ designs by Jungnickel and Vanstone (1986). In Section 3 we investigate the conditions under which the designs obtained by the basic construction are simple. Many infinite families of simple 3-designs are presented, which are closely related to some familiar families, including those found by Iwasaki and Meixner [22], Laue [28], and van Tran [40,41]. On the other hand, the designs obtained by the basic construction possess various properties. In Section 4 a theory of constructing simple cyclic 3-$(v,4,3)$ designs by Köhler [26] and its abelian-group extension by Munemasa and Sawa [35] are readily rebuilt from the context of this paper. In Section 5 many infinite families of simple resolvable 3-designs are presented, in comparison with known families of Laue [28] and van Tran [41]. We also show that for any prime power q and any odd integer n there exists a resolvable 3-$(q^n+1, q+1, 1)$ design. As far as the authors know, this is the first and the only known infinite family of resolvable t-$(v,k,1)$ designs with $t \geqslant 3$ and $k \geqslant 5$. We emphasize that those resolvable 3-designs could be applied to the basic construction again.

2. Basic construction

In this section we describe a construction of 3-designs by using the resolvability of a 3-design. The importance of the basic construction will become clear in the following sections.

A t-design with v points and blocks of size k is said to have a *resolution* if its blocks can be partitioned into classes, called *resolution classes*, each of which consists of v/k pairwise disjoint blocks. A design is said to be *resolvable* if it has a resolution. In the field of geometry, a parallelism or a parallel class is often used instead of a resolution or a resolution class respectively. We refer the reader to [12] for the details of these terminologies.

Let $\mathcal{D} = (V, \mathcal{B})$ be a t-(v,k,λ) design. It is well known (see, e.g., [9]) that for each integer $0 \leqslant t' \leqslant t$ and a t'-subset T' of V, $|\{B \in \mathcal{B} \mid T' \subset B\}|$ is a constant, say $b_{t'}^{(\mathcal{D})}$, which does not depend on the choice of T'. In particular, note that $b_t^{(\mathcal{D})} = \lambda$ and $b_0^{(\mathcal{D})} = |\mathcal{B}|$. For our convenience we regard a t'-$(v, t', 1)$ design as a t-design such that $b_i^{(\mathcal{D})} = 0$ for each integer i with $t' < i \leqslant t$.

Theorem 2.1. *Let k_1, k_2, v_1, v_2 be positive integers such that $v_1 = v_2 k_1$ and $k_2 \leqslant v_2/2$. Assume that there exist a resolvable 3-(v_1, k_1, λ_1) design $\mathcal{D}_1$ and a 3-(v_2, k_2, λ_2) design $\mathcal{D}_2$. Then there exists a 3-$(\widetilde{v}, \widetilde{k}, \widetilde{\lambda})$ design $\widetilde{\mathcal{D}}$, where*

$$\widetilde{v} = v_1, \qquad \widetilde{k} = k_1 k_2,$$
$$\widetilde{\lambda} = b_3^{(\mathcal{D}_1)} b_1^{(\mathcal{D}_2)} + 3\big(b_2^{(\mathcal{D}_1)} - b_3^{(\mathcal{D}_1)}\big) b_2^{(\mathcal{D}_2)} + \big(b_1^{(\mathcal{D}_1)} - 3b_2^{(\mathcal{D}_1)} + 2b_3^{(\mathcal{D}_1)}\big) b_3^{(\mathcal{D}_2)}.$$

Proof. Let $\mathcal{D}_1 = (V, \mathcal{B}_1)$. Note that the number of resolution classes in $\mathcal{D}_1$ equals $b_1^{(\mathcal{D}_1)}$. Let $\mathcal{R} = \{R_1, \ldots, R_{b_1^{(\mathcal{D}_1)}}\}$ be a resolution of $\mathcal{D}_1$ and $R_j = \{B_x^{(j)} \mid x = 1, \ldots, v_2\}$. Regard $\mathcal{D}_2$ as a 3-(v_2, k_2, λ_2) design with points $\{1, \ldots, v_2\}$ and blocks $\mathcal{B}_2$. We claim that the incidence structure on V defined by

$$\widetilde{\mathcal{B}} = \left\{ \bigcup_{x \in B} B_x^{(j)} \;\middle|\; B \in \mathcal{B}_2,\ j = 1, \ldots, b_1^{(\mathcal{D}_1)} \right\}$$

is a 3-design with the desired parameters. Let T be a triple of V. Every block $\widetilde{B} = \bigcup_{x \in B} B_x^{(j)}$ which contains T has either one of the following forms:

(i) $T \subset B_x^{(j)}$ for some x.
(ii) $T \subset B_x^{(j)} \cup B_{x'}^{(j)}$, $T \cap B_x^{(j)} \neq \emptyset$, $T \cap B_{x'}^{(j)} \neq \emptyset$ for some distinct x, x'.
(iii) $T \subset B_x^{(j)} \cup B_{x'}^{(j)} \cup B_{x''}^{(j)}$, $T \cap B_x^{(j)} \neq \emptyset$, $T \cap B_{x'}^{(j)} \neq \emptyset$, $T \cap B_{x''}^{(j)} \neq \emptyset$ for some distinct x, x', x''.

By the principle of inclusion and exclusion, we see that the total number of blocks of type (i) or type (ii) or type (iii) respectively equals $b_3^{(\mathcal{D}_1)} b_1^{(\mathcal{D}_2)}$ or $3(b_2^{(\mathcal{D}_1)} - b_3^{(\mathcal{D}_1)}) b_2^{(\mathcal{D}_2)}$ or $(b_1^{(\mathcal{D}_1)} - 3b_2^{(\mathcal{D}_1)} + 2b_3^{(\mathcal{D}_1)}) b_3^{(\mathcal{D}_2)}$, which completes the proof. $\square$

Hereafter we say that $\mathcal{D}_1, \mathcal{D}_2, \widetilde{\mathcal{D}}$ given in Theorem 2.1 are respectively *master design*, *embedding design*, *composed design*.

Remark 2.2. The basic construction presented in Theorem 2.1 extends a well-known construction of 3-designs with block size 4 by Jungnickel and Vanstone [25] to that of 3-designs with general block sizes.

3. Simplicity

In this section we investigate the conditions under which composed designs by the basic construction discussed in Section 2 are simple. For this purpose, a master design and an embedding design must be necessarily simple, however these requirements are not enough to make the composed design simple. Here we look at some sufficient conditions for a composed design to be simple.

3.1. The case $k_1 = 2$

We assume that v is an even positive integer and a master design is a 2-$(v, 2, 1)$ design. It is well known (see, e.g., [5,7]) that a 2-$(v, 2, 1)$ design is resolvable. Conditions under which composed designs are simple can be graph-theoretically formulated.

Let K_v be the complete graph of a v-element set of vertices V. A 1-*factorization* $\mathcal{F}$ of K_v is a partition of the edge-set into $v - 1$ classes $F_1, \ldots, F_{v-1}$, called 1-*factors*, each of which is a partition of V. For a subset $\mathcal{L}$ of $\{1, \ldots, v-1\}$, the subgraph $\bigcup_{l \in \mathcal{L}} F_l$ consists of vertices V and those edges in F_i, $i \in \mathcal{L}$. This is called an *α-factor generated from $\mathcal{F}$* if $|\mathcal{L}| = \alpha$; the notation $|\cdot|$ will be also used to denote the order of a finite group or the order of an element of a finite group, but the reader will see what it means from the context. Any 2-factor generated from $\mathcal{F}$ is determined up to isomorphisms by the lengths of its cycles. A classical problem in combinatorics and geometry is to find a 1-factorization of K_v for which any generated 2-factor has the same cycle structure [3]. In particular, if any generated 2-factor is isomorphic to Hamiltonian cycle, then a 1-factorization is said to be *perfect*. Another direction of research is to find a 1-factorization $\mathcal{F}$ of K_v for which any generated 2-factor contains no cycle of a given length; for example, see [33]. $\mathcal{F}$ is said to be *ℓ-cycle free* if any 2-factor generated from $\mathcal{F}$ forbids a cycle of length ℓ. More generally, we introduce the following concept: $\mathcal{F}$ is said to be *ℓ-union free* if the union of cycles from any 2-factor can never have size ℓ.

Now, let us identify a 1-factorization of K_v with a resolution of a 2-$(v, 2, 1)$ design. The following makes clear the importance of the concept of the ℓ-union freeness.

Theorem 3.1. *Assume ℓ is an even integer, $\mathcal{D}_1$ is ℓ-union free and $\mathcal{D}_2$ is simple. Then $\widetilde{\mathcal{D}}$ is simple.*

Proof. Straightforward. □

Let us consider the existence problem of an ℓ-union free 1-factorization of a complete graph. First, observe that if $\ell \in \{4, 6\}$, the existence of an ℓ-cycle free 1-factorization is equivalent to that of an ℓ-union free 1-factorization. The following are due to Jungnickel and Vanstone [25], Meszka [32], Phelps, Stinson and Vanstone [37].

Theorem 3.2.

(i) *(See [25,37].) For every even integer v, there exists a 4-cycle free 1-factorization of K_v.*
(ii) *(See [32].) For every even integer v such that $v \equiv 2 \pmod 4$, there exists a 6-cycle free 1-factorization of K_v.*

The problem becomes more involved when $\ell \geqslant 8$: In this case, in order to investigate the cycle structure of any generated 2-factor in detail, it is convenient to assume that a master design has a certain algebraic structure. Let A be a finite abelian group. A 1-factorization of K_v on vertices $A \cup \{\infty\}$ can be defined by

$$F_a = \bigl\{\{\infty, a\}\bigr\} \cup \left\{\{b, c\} \in \binom{A}{2} \;\middle|\; 2a = b + c\right\}, \quad a \in A.$$

Here $\binom{A}{d}$ denotes the set of all d-subsets of A, and the operation in A is additively written. This 1-factorization is denoted by GK_v. It is well known [12] that for distinct $a, a' \in A$, the 2-factor $F_a \cup F_{a'}$ of GK_v consists of an $(m+1)$-gon (containing ∞) and a number of $2m$-gons such that the order of $a - a'$ is m.

Theorem 3.3. *Let v, ℓ be even positive integers such that* $\gcd(\ell/2, v-1) = \gcd(\ell-1, v-1) = 1$. *Then GK_v is ℓ-union free.*

Proof. Assume a 2-factor generated from GK_v induces a subgraph with ℓ vertices. Then for some divisor m of $v-1$, it consists of $2m$-gons only, or a number of $2m$-gons and an $(m+1)$-gon (containing ∞). In the former case ℓ is divisible by $2m$, whereas in the latter case, $\ell - 1$ is divisible by m. □

A 1-factorization $\mathcal{F}$ of the complete graph on vertices A is said to be *A-invariant* if for any $a \in A$, $F \in \mathcal{F}$ implies $F + a \in \mathcal{F}$, where $F + a = \{\{b + a, b' + a\} \mid \{b, b'\} \in F\}$. In particular if A is cyclic, this is said to be *cyclic*. The set $\{F + a \mid a \in A\}$, denoted by $\mathrm{Orb}_A(F)$, is the *A-orbit* of a 1-factor F. Hartman and Rosa [20] showed that for any v which is not a power of 2, there exists a cyclic 1-factorization of K_v. When $v \equiv 2 \pmod 4$, this 1-factorization is isomorphic to the well-known 1-factorization GA_v [4]. Identifying A with the set $\mathbb{Z}_v$ of residue classes modulo v, we can represent GA_v as a collection of the $\mathbb{Z}_v$-orbits of the following 1-factors:

$$F = \bigl\{\{0, v/2\}\bigr\} \cup \bigl\{\{b, -b\} \bigm| b = 1, \ldots, (v-2)/2\bigr\},$$
$$F_{2a-1} = \bigl\{\{2b, 2a+2b-1\} \bigm| b = 0, \ldots, (v-2)/2\bigr\}, \quad a = 1, \ldots, (v-2)/4;$$

see Hartman and Rosa [20]. Meszka [32, Lemma 6] showed that for an even integer ℓ such that $4 \leqslant \ell \leqslant v$ and $v \not\equiv 0 \pmod{\ell/2}$, GA_v is ℓ-cycle free. Therefore if $v \not\equiv 0 \pmod{\ell'/2}$ for every even integer ℓ' such that $4 \leqslant \ell' \leqslant \ell$, then we see that GA_v is ℓ-union free.

In comparison with the above Meszka-type condition, we can obtain a better sufficient condition for GA_v to be ℓ-union free. Let $v \geqslant 6$ be a positive integer such that $v \equiv 2 \pmod 4$. Let A be an abelian group of order v. Then A contains a unique element h of order 2. Let f be the group endomorphism of A defined by $f(a) = 2a$. Let $f(A)$, $\ker(f)$ be respectively the image and kernel of f, that is, $f(A) = \{f(a) \mid a \in A\}$, $\ker(f) = \{a \mid f(a) = 0\}$. Then we readily see that the A-orbits of the 1-factors

$$F = \bigl\{\{0, h\}\bigr\} \cup \bigl\{\{b, -b\} \bigm| b \in A \setminus \{0, h\}\bigr\},$$
$$F_a = \bigl\{\{b, a+b\} \bigm| b \in f(A)\bigr\}, \quad a \in A \setminus \bigl(f(A) \cup \{h\}\bigr) \tag{1}$$

form an A-invariant 1-factorization of K_v. This is called $\widetilde{GA_v}$. Note that $\widetilde{GA_v}$ is a simple extension of GA_v to an arbitrary abelian group. We investigate the cycle structure of $\widetilde{GA_v}$ instead of GA_v, which will be useful for discussion in Section 4.

Assume an abelian group A acts regularly on points V. Then we can identify V with A. For a subset B of V and an element a of A, we let $B + a = \{b + a \mid b \in B\}$. The following lemma is useful for further arguments later.

Lemma 3.4. *Let V be a finite set of cardinality v on which an abelian group A acts regularly. If a subset B of V satisfies $B = B + a$ for some $a \in A$, then $|B| \equiv 0 \pmod{|a|}$.*

Proof. The result follows by noting that B decomposes into cycles of a of size $|a|$. $\square$

Theorem 3.5. *Let v, ℓ be even integers such that $v \equiv 2 \pmod 4$, $\ell \geqslant 4$ and $\gcd(\ell/2, v/2) = 1$. Then $\widetilde{GA_v}$ is ℓ-union free.*

Proof. Assume there exist two distinct 1-factors F', F'' such that $\bigcup_{e \in B'} e = \bigcup_{e \in B''} e$ for some $B' \subset F'$, $B'' \subset F''$, $|B'| = |B''| = \ell/2$, where $\bigcup_{e \in B'} e$ or $\bigcup_{e \in B''} e$ is not a set of edges, but a set of vertices. The proof consists of three cases.

Case 1. $F', F'' \in \mathrm{Orb}_A(F)$.

In this case for some nonzero element $a \in A$ we have $F' = F'' + a$. F' and F'' are distinct, so that $a \notin \{0, h\}$. Without loss of generality we may assume $F' = F$ and therefore $F' = -F'$, $F'' = -F'' - 2a$. This implies that

$$\bigcup_{e \in B'} e = \bigcup_{e \in B''} e = -\Bigl(\bigcup_{e \in B''} e\Bigr) - 2a = -\Bigl(\bigcup_{e \in B'} e\Bigr) - 2a = \Bigl(\bigcup_{e \in B'} e\Bigr) - 2a.$$

Thus by Lemma 3.4 we have $|\bigcup_{e \in B'} e| \equiv 0 \pmod{|2a|}$, contradicting the assumption $\gcd(\ell/2, v/2) = 1$.

Case 2. $F' \in \mathrm{Orb}_A(F)$, $F'' \in \mathrm{Orb}_A(F_a)$ for some $a \in A \setminus (f(A) \cup \{h\})$.

Without loss of generality we may assume $F' = F$. Then

$$\Big(\bigcup_{e\in B''} e\Big)\cap f(A) = -\Big(\Big(\bigcup_{e\in B''} e\Big)\cap f(A)\Big),$$
$$\Big(\bigcup_{e\in B''} e\Big)\cap \big(A\setminus f(A)\big) = -\Big(\Big(\bigcup_{e\in B''} e\Big)\cap \big(A\setminus f(A)\big)\Big).$$

We may assume $F'' = F_a$ or $F'' = F_a + a$, since F_a is invariant under $f(A)$, that is, $F_a + b = F_a$ for any $b \in f(A)$. In the former case, we have

$$\Big(\Big(\bigcup_{e\in B''} e\Big)\cap f(A)\Big) + a = \Big(\bigcup_{e\in B''} e\Big)\cap \big(A\setminus f(A)\big).$$

Therefore

$$\begin{aligned}\Big(\bigcup_{e\in B''} e\Big)\cap f(A) &= -\Big(\Big(\bigcup_{e\in B''} e\Big)\cap f(A)\Big) = -\Big(\Big(\bigcup_{e\in B''} e\Big)\cap \big(A\setminus f(A)\big)\Big) + a\\ &= \Big(\Big(\bigcup_{e\in B''} e\Big)\cap \big(A\setminus f(A)\big)\Big) + a = \Big(\Big(\bigcup_{e\in B''} e\Big)\cap f(A)\Big) + 2a.\end{aligned}$$

Hence by Lemma 3.4 we have $|\bigcup_{e\in B''} e| \equiv 0 \pmod{|2a|}$, which is a contradiction. A similar argument is also valid for the case where $F'' = F_a + a$.

Case 3. $F' \in \mathrm{Orb}_A(F_a)$, $F'' \in \mathrm{Orb}_A(F_{a'})$ for some $a, a' \in A\setminus(f(A)\cup\{h\})$.

Without loss of generality we may assume $F' = F_a$, and $F'' = F_{a'}$ or $F'' = F_{a'} + a'$. If $F'' = F_{a'}$, then

$$\begin{aligned}\Big(\Big(\bigcup_{e\in B'} e\Big)\cap f(A)\Big) + a &= \Big(\bigcup_{e\in B'} e\Big)\cap \big(A\setminus f(A)\big) = \Big(\bigcup_{e\in B''} e\Big)\cap \big(A\setminus f(A)\big)\\ &= \Big(\Big(\bigcup_{e\in B''} e\Big)\cap f(A)\Big) + a' = \Big(\Big(\bigcup_{e\in B'} e\Big)\cap f(A)\Big) + a'.\end{aligned}$$

By Lemma 3.4 we have $|\bigcup_{e\in B'} e| \equiv 0 \pmod{|a' - a|}$, which is a contradiction. A similar argument also works when $F'' = F_{a'} + a'$. $\square$

Combining the preceding results, we get the following.

Theorem 3.6. *Let v, ℓ be even positive integers with $2\ell \leqslant v$. Assume there exists a simple 3-design with $v/2$ points and blocks of size $\ell/2$, say $\mathcal{D}_2$. Then, with the same notations $b_2^{(\mathcal{D}_2)}, b_3^{(\mathcal{D}_2)}$ as in Section 2, there exists a simple 3-$(v, \ell, 3b_2^{(\mathcal{D}_2)} + (v-4)b_3^{(\mathcal{D}_2)})$ design if one of the following conditions is satisfied:*

(i) $\ell = 4$, *or* $\ell = 6$ *and* $v \equiv 2 \pmod 4$.
(ii) $\gcd(\ell - 1, v - 1) = \gcd(\ell/2, v - 1) = 1$.
(iii) $\gcd(\ell/2, v/2) = 1$ *and* $v \equiv 2 \pmod 4$.

Proof. By applying Theorem 2.1 to a 2-$(v, 2, 1)$ design as a master design and $\mathcal{D}_2$ as an embedding design, we obtain a 3-$(v, \ell, 3b_2^{(\mathcal{D}_2)} + (v-4)b_3^{(\mathcal{D}_2)})$ design. In particular when a 2-$(v, 2, 1)$ design is taken to be that given in Theorem 3.2, Theorem 3.3, Theorem 3.5, the composed design is simple by Theorem 3.1. $\square$

Later in Section 3.3, we will present many infinite families of simple 3-designs that are obtained by Theorem 3.6, in comparison with some familiar families.

We close this subsection by giving the reader notice that any perfect 1-factorization can be considered as an ℓ-union free 1-factorization. The conjecture by Kotzig [27] states that a perfect 1-factorization of K_v exists for every order v. Though only a few infinite families were found (e.g., see [12]), many sporadic examples of perfect 1-factorizations of small orders are found by computer search. The following is a list of small orders for which sporadic examples of perfect 1-factorizations are known [6]:

16, 28, 36, 40, 50, 126, 170, 244, 344, 530, 730, 1332, 1370, 1850, 2198, 2810,

3126, 4490, 6860, 6890, 11 450, 11 882, 12 168, 15 626, 16 808, 22 202, 24 390,

24 650, 26 570, 29 792, 29 930, 32 042, 38 810, 44 522, 50 654, 51 530, 52 442,

63 002, 72 362, 76 730, 78 126, 79 508, 103 824, 148 878, 161 052, 205 380,

226 982, 300 764, 357 912, 371 294, 493 040, 571 788, 1 092 728, 1 225 044.

These perfect 1-factorizations generate simple 3-designs.

3.2. The case $k_1 > 2$

In this subsection a sufficient condition for a 3-design obtained by the basic construction to be simple is presented in terms of block intersections of two blocks in different resolution classes of a master design.

Theorem 3.7. *Assume $\mathcal{D}_1$ has index* 1 *and $\mathcal{D}_2$ is simple. If $k_1 \geqslant 2k_2 + 1$, then $\widetilde{\mathcal{D}}$ is simple.*

Proof. We use the same notations as in the proof of Theorem 2.1. In order to show the simplicity of $\widetilde{\mathcal{D}}$, we must check that $\bigcup_{x\in B} B_x^{(j)} \neq \bigcup_{y\in B'} B_y^{(j')}$ holds for $j, j' = 1, \ldots, b_1^{(\mathcal{D}_1)}$, $B, B' \in \mathcal{B}_2$, $(j, B) \neq (j', B')$. Assume contrary. When $j = j'$, this trivially contradicts the construction of $\widetilde{\mathcal{D}}$. When $j \neq j'$, it follows that for any $x \in B$,

$$\left| B_x^{(j)} \cap \left(\bigcup_{y\in B'} B_y^{(j')} \right) \right| = \sum_{y\in B'} \left| B_x^{(j)} \cap B_y^{(j')} \right| \leqslant 2k_2.$$

Here the last inequality sign follows by noting any two blocks of a Steiner 3-design intersect in at most 2 points. This is a contradiction to the assumption $k_1 \geqslant 2k_2 + 1$. The proof is complete. □

Remark 3.8. Rahilly [38] investigated the conditions under which 2-designs can be constructed as the union of certain sets of blocks of known 2-designs. This method is known as the union method and generally requires that the design we start with should possess a dual property. The idea of the union method is to take unions of pairs of blocks in different classes of the affine resolution of an affine resolvable 2-design. If the number of blocks in such a class equals two, the constructed 2-design is also a 3-design. Rahilly presented necessary and sufficient conditions for such a 3-design to be simple. These conditions are stated in terms of block intersection numbers of blocks in different classes of an affine resolution. In this sense Theorem 3.7 is similar to the union method by Rahilly.

By using Theorem 3.7, we can actually obtain some simple 3-designs.

Example 3.9. (i) Let $\mathcal{D}_1$ be a resolvable 3-$(q^3+1, q+1, 1)$ design; such a design exists (see Theorem 5.4(i) later). Let $\mathcal{D}_2$ be a simple 3-(q^2-q+1, k_2, λ) design. If $q+1 \geqslant 2k_2+1$, then there exists a simple 3-$(q^3+1, k_2(q+1), \widehat{\lambda})$ design for some $\widehat{\lambda}$ to be calculated. A small λ for q^2-q+1 points is known for sporadic cases. For example when $q = 7$, then there is a simple 3-$(43, 4, 4)$ design admitting $Hol(C_{43})$, the semidirect product of C_{43} with its automorphism group C_{42}. So there is a simple 3-$(344, 32, \lambda)$ design. It might be interesting to generalize this construction for a prime number of the form q^2-q+1.

Table 1
Families of simple 3-designs by Theorem 3.6.

No.	$\mathcal{D}_2$	$\widetilde{\mathcal{D}}$	Conditions
1	2-$(v/2, 2, 1)$	3-$(v, 4, 3)$	$v \equiv 0 \pmod 2$
2	3-$(v/2, 3, 1)$	3-$(v, 6, 5(v-4)/2)$	$v \equiv 2 \pmod 4$
3	3-$(v/2, 4, 1)$ (Hanani [17])	3-$(v, 8, 7(v-4)/4)$	$v \equiv 4$ or $8 \pmod{12}$, $v \not\equiv 1 \pmod 7$
4	3-$(v/2, v/4, (v-8)/8)$ (Hadamard Type)	3-$(v, v/2, (v-4)(v-2)/8)$	$\exists H(v/2)$
5	3-$(v/2, v/4, (v-8)/4)$ (Driessen [15])	3-$(v, v/2, (v-4)(v-2)/4)$	$\exists H(v)$ and $v \equiv 4 \pmod 8$ or $v/2-1$ is a prime power
6	3-$(3^{2n}+1, 3^n+1, 1)$ (Circle geometry)	3-$(3^{2n}2+2, 3^n2+2, (3^n2+1)(3^n+1))$	
7	3-$(q^n+1, q+1, 1)$ (Spherical geometry)	3-$(2q^n+2, 2q+2, 2q^n+3\frac{q^n-1}{q-1}-2)$	q is a prime power $n \equiv 1 \pmod 2$ $\gcd(2q^n+1, 2q+1)=1$
8	$\widetilde{\mathcal{D}}$ of No. 3	3-$(v, 16, 35(v-4)(v-8)/32)$	$v \equiv 8$ or $16 \pmod{24}$, $v \not\equiv 1 \pmod 7$, $\gcd(v-1, 15)=1$

(ii) There are infinite families of 3-designs with rather large index, resulting from Large Set recursion. There exist Large Sets $LS[3](3, k, v)$ for $k = 8$ and $v \equiv 3, 4, 5, 6, 7 \pmod 9$, $v > 11$. Each of these consists of three 3-$(v, 8, \frac{1}{3}\binom{v-3}{8-3})$ designs. If $q \equiv 2, 3, 4, 5, 6, 7, 8 \pmod 9$, then q^2-q+1 belongs to these congruence classes. So, if $q+1 > 16$ there is a simple 3-$(q^3+1, 8(q+1), \lambda)$ design for a nasty λ. This idea can be applied also for $k = 5, 6, 7$ with fewer possibilities for v. There exist Large Sets $LS[7](3, k, v)$ for $k = 6$ and $v \equiv 3, 4, 5 \pmod 7$, $v > 16$. Each of these consists of seven 3-$(v, 6, \frac{1}{7}\binom{v-3}{6-3})$ designs. Also, there are further infinite families of Large Sets of 3-designs where λ is smaller. We can also use the theorem of Mohacsy and Ray-Chaudhuri [34]: If for a prime power p^r and a positive integer $a \geqslant 2$, the parameter set 3-$(a^n v+1, p^r+1, 1)$ is admissible and n is sufficiently large then there exists a Steiner system with these parameters. We consider cases where $q^2-q+1 = a^n v+1$. The condition is equivalent to $q(q-1) = a^n v$. So, for $q = p^f$ and $a^n = p^r < q$ we have $v = p^{f-r}(p^f-1)$. Then, for admissible large enough parameters there exist 3-$(q(q-1), p^r+1, 1)$ designs. Combining such a design with the resolvable 3-$(q^3+1, q+1, 1)$ design using Theorem 3.7, we obtain a simple 3-$(p^{3f}+1, (p^r+1)(p^f+1), \lambda)$ design. On the other hand, in a recent application to quantum jump codes (e.g., see [1,2]), a collection of disjoint t-designs play an important role. Our construction in Theorem 3.7 may be applied to obtain such disjoint t-designs.

3.3. New families

Theorem 3.6 generates many infinite families of 3-designs. In this subsection we exhibit some of them (see Table 1) that are related to some familiar families by Iwasaki and Meixner [22], Jungnickel and Vanstone [25], Laue [28], Phelps, Stinson and Vanstone [37], van Tran [40,41]. All designs considered in this subsection are simple.

In Table 1, "Conditions" implies the conditions under which each $\widetilde{\mathcal{D}}$ is simple. $H(v/2)$ means a Hadamard matrix of order $v/2$. Nos. 1 and 2 are obtained by Theorem 3.6(i) and the others by (ii).

We close this subsection by the following observations.

(i) Up to isomorphisms, No. 1 is equivalent to that of Jungnickel and Vanstone [25] and Phelps, Stinson and Vanstone [37].

(ii) Nos. 2 and 3 extensively generalize three infinite families by van Tran [41, Theorem 2.4, Theorem 2.5], that is, a 3-$(2^{m+1}+2, 6, 5(2^m-1))$ design, a 3-$(2^n 20, 8, 7(2^{n-2}20-1))$ design, a 3-$(2^n 28, 8, 7(2^{n-2}28-1))$ design, where $m \geqslant 5$ is an odd integer and $n \geqslant 0$ is an integer.

(iii) In comparison with a family of Laue [28, Theorem 3.1], that is, a 3-$(q+1, (q+1)/2, (q-1)(q-3)/8)$ design, where $q > 5$ is an odd prime power, No. 4 has more general parameters. Many families can be obtained by several known families of Hadamard matrices; for example see [30] for a collection of known Hadamard matrices.

(iv) Iwasaki and Meixner [22] found a 3-$(q+1, (q+1)/2, (q+1)(q-3)/8)$ design for every prime power $q \equiv 3 \pmod 4$. Their family belongs to a class of 3-$(v, v/2, v(v-4)/8)$ designs whose index is larger than that of the design of No. 4. On the other hand, van Tran [41, Theorem 2.13, Theorem 2.14] found a 3-$(2^i 24, 8, 21(2^{i-2}24-1))$ design, a 3-$(2^i 48, 16, 105(2^{i-2}48-1)(2^{i-3}48-1))$ design, where $i \geqslant 0$ is an integer. These families belong to a class of 3-$(v, 8, 21(v-4)/4)$ designs and 3-$(v, 16, 105(v-4)(v-8)/32)$ designs, whose indices are three times larger than those of Nos. 3 and 8 respectively.

(v) Nos. 6 and 7 are interesting because infinite families of 3-designs which have $O(v^2)$ index and non-constant block size k on v are rare.

4. Reconstruction of Köhler's theory

In this section we show that the basic construction discussed in Section 2 can be applied to construct 3-designs admitting an abelian group as a point-regular automorphism group. As a by-product, we give an alternative proof of a theorem by Köhler [26] which states that for every positive integer $v \equiv 2 \pmod 4$, there exists a simple 3-$(v, 4, 3)$ design with point-cyclic automorphism group. All designs considered in this section are simple.

We start with the following easy result.

Theorem 4.1. *With the same notation as in Theorem* 2.1, *we assume $\mathcal{D}_1$ admits a group G as a point-regular automorphism group and $\mathcal{D}_2$ is a complete design. Then $\widetilde{\mathcal{D}}$ admits G as a point-regular automorphism group.*

Proof. Straightforward. $\square$

Hereafter we let A be an abelian group of order v. Let $\widehat{A}$ denote the semidirect product $A \rtimes \langle\sigma\rangle$, where σ is the permutation of A such that $a^\sigma = -a$. A k-subset B of A is said to be a *symmetric k-block* if it is fixed by an element of $\widehat{A}$ not in A:

$$B = -B + x \quad \text{for some } x \in A. \tag{2}$$

The definition of a symmetric k-block generalizes that of a *symmetric k-difference cycle* which was introduced by Köhler [26] for $A \simeq \mathbb{Z}_v$. To see this, regard the elements of $\mathbb{Z}_v$ as integers $0 \leqslant j < v$. To a k-subset $B = \{b_1, \dots, b_k\}$ of $\mathbb{Z}_v$ with $0 \leqslant b_1 < b_2 < \cdots < b_k < v$, we associate a *cycle* $c = (c_1, c_2, \dots, c_k)$, where $c_i = b_{i+1} - b_i$ for $1 \leqslant i < k$, $c_k = b_1 - b_k$. Then, a translate of B corresponds to a cyclic shift of c, whereas, $-B$ corresponds to $(c_{k-1}, \dots, c_1, c_k)$ or $(c_k, \dots, c_1)$, according to $b_1 = 0$ or not. Köhler calls $c = (c_1, \dots, c_k)$ a *symmetric k-difference cycle*, if c is a cyclic shift of $(c_k, \dots, c_1)$. It is easy to see that B satisfies (2) if and only if the corresponding cycle is a symmetric k-difference cycle. He proved that for every $v \equiv 2 \pmod 4$, the set of all 4-subsets corresponding to symmetric 4-difference cycles generates a simple 3-$(v, 4, 3)$ design with $\mathbb{Z}_v$ as a point-regular automorphism group. This theorem was recently extended to an arbitrary abelian group:

Theorem 4.2. *(See [35].) For any positive integer $v \equiv 2 \pmod 4$ and any abelian group A of order v, the set of all symmetric* 4*-blocks generates a simple* 3-$(v, 4, 3)$ *design with A as a point-regular automorphism group.*

For $v \equiv 2 \pmod 4$, let us consider a simple 3-$(v, 4, 3)$ design with A as a point-regular automorphism group which is constructed from $\widetilde{GA}_v$ in Section 3. The following states that these designs are equivalent to those obtained from Theorem 4.2.

Theorem 4.3. *Let $v \equiv 2 \pmod 4$ and A be an abelian group of order v. Then the* 3-$(v, 4, 3)$ *design constructed by Theorem* 3.6(iii) *with $\widetilde{GA}_v$ is equivalent to that of Theorem* 4.2 *up to isomorphisms.*

Proof. Let f, h be the mappings used in (1). It is known [35] that the set of all symmetric 4-blocks can be partitioned into two disjoint sets

$$\mathcal{B}_0 = \bigl\{\{0, a, b, a+b\} + c \bigm| a, b \in A \setminus \{0\},\ c \in A,\ a \neq \pm b\bigr\},$$
$$\mathcal{B}_1 = \bigl\{\{0, h, a, -a\} + c \bigm| a \in A \setminus \{0, h\},\ c \in A\bigr\}.$$

Any block B of the design constructed by Theorem 3.6(iii) with $\widetilde{GA}_v$ is a translate of a block which has one of the following forms:

(i) $\{0, a, b, a+b\}, \quad a \in A \setminus \bigl(f(A) \cup \{h\}\bigr),\ b \in f(A) \setminus \{0\},$

(ii) $\{0, h, a, -a\}, \quad a \in A \setminus \{0, h\},$

(iii) $\{a, -a, b, -b\}, \quad a, b \in A \setminus \{0, h\},\ a \neq \pm b.$

If the first two cases occur, then it is obvious that $B \in \mathcal{B}_0 \cup \mathcal{B}_1$. Next assume that the third case occurs, that is, $B = \{a, -a, b, -b\} + c$ for some $a, b \in A \setminus \{0, h\}$, $a \neq \pm b$, $c \in A$. Then

$$\{a, -a, b, -b\} + c = \{0, b-a, b+a, 2b\} + (c-b) \in \mathcal{B}_0,$$

since $0 \notin \{2a, 2b\}$. □

Remark 4.4. The original proof of Theorem 4.2 by Munemasa and Sawa [35] uses combinatorial arguments, and is 3 pages long. Theorem 4.3 gives an alternative short proof using the resolvability, and implies that the basic construction discussed in Section 2 extends the theories by Köhler, and Munemasa and Sawa to 3-designs with general block sizes.

5. Resolvability

In this section we show that the basic construction discussed in Section 2 can be applied to construct resolvable 3-designs. Many infinite families are presented, in comparison with known families that were found by Laue and van Tran. All designs considered in this section are simple.

To construct resolvable 3-designs is one of the hardest problems in design theory. It is usual to use $\mathrm{PGL}(2,q)$ or $\mathrm{PSL}(2,q)$; for example see [8,28]. The basic idea is to first prescribe a stabilizer U of a block B and then an overgroup H of U which maps B onto disjoint copies, and thereby to partition the points on the projective line. This method in fact generates many resolvable 3-designs; for example see [28]. On the other hand, van Tran's recursive constructions for simple 3-designs which already appear in Section 3.3 can also apply to construct resolvable 3-designs. We refer the reader to the original papers by van Tran [40,41] for details. There are some other constructions for 3-designs with block size 4, however as far as the authors know, the group-theoretic approach and van Tran's recursive approach seem to be the only known methods to construct resolvable 3-designs with general block sizes. The following construction is different from these elementary constructions.

Theorem 5.1. *With the same notation as in Theorem* 2.1, *we assume $\mathcal{D}_2$ is resolvable. Then $\widetilde{\mathcal{D}}$ is resolvable.*

Proof. Straightforward. □

Remark 5.2. Theorem 5.1 generalizes a construction of resolvable 3-designs with block size 4 by Jungnickel and Vanstone [25] which already appears many times in the previous sections.

Theorem 5.1 can generate many infinite families of resolvable 3-designs.

Theorem 5.3.

(i) *Let v be a positive integer such that* $v \equiv 6 \pmod{12}$. *Then there exists a resolvable* $3\text{-}(v, 6, 5(v-4)/2)$ *design.*
(ii) *Let v be a positive integer such that $v \equiv 8$ or* $16 \pmod{24}$ *and* $v \not\equiv 1 \pmod 7$. *Then there exists a resolvable* $3\text{-}(v, 8, 7(v-4)/4)$ *design.*
(iii) *Assume there exists a Hadamard matrix of order $v/2$. Then there exist a resolvable* $3\text{-}(v, v/2, (v-4)(v-2)/8)$ *design and a resolvable* $3\text{-}(v, v/2, (v-4)(v-2)/4)$ *design.*

Proof. We use the same notation and terminology as in Section 3.3.

(i) No. 2 is obtained by taking a $3\text{-}(v/2, 3, 1)$ design to be $\mathcal{D}_2$. By Baranyai's theorem [7], $\mathcal{D}_2$ is resolvable if $v \equiv 0 \pmod 3$. The result thus follows by Theorem 5.1.

(ii) It is known [18,23] that there exists a resolvable $3\text{-}(v/2, 4, 1)$ design, say $\mathcal{D}_2$, for every positive integer $v \equiv 8$ or $16 \pmod{24}$ and $v \not\equiv 1 \pmod 7$. By applying Theorem 3.6(ii) to $\mathcal{D}_2$, we obtain a simple $3\text{-}(v, 8, 7(v-4)/4)$ design, which is resolvable by Theorem 5.1.

(iii) Nos. 4 and 5 are obtained by taking a Hadamard 3-design as an embedding design. Any Hadamard 3-design is resolvable (e.g., see [5]). Therefore the result follows by Theorem 5.1. □

More infinite families of resolvable 3-designs can be obtained using a classical construction.

Theorem 5.4.

(i) *Let q be a prime power and n be a positive integer. Then there exists a resolvable* $3\text{-}(q^n+1, q+1, 1)$ *design if and only if* $n \equiv 1 \pmod 2$.
(ii) *With the same q^n as in* (i), *if* $\gcd(2q+1, 2q^n+1) = 1$, *then there exists a resolvable* $3\text{-}(2q^n+2, 2q+2, 2q^n + 3\frac{q^n-1}{q-1} - 2)$ *design.*

Proof. (i) Let $G = \mathrm{PGL}(2, q^n)$. It is well known (see, e.g., Witt [43]) that there exists a $3\text{-}(q^n+1, q+1, 1)$ design, say $\mathcal{D}$, admitting G as an automorphism group. We show that $\mathcal{D}$ is resolvable, if $n \equiv 1 \pmod 2$.

We review the construction of $\mathcal{D}$. The group G contains a subgroup H isomorphic to $\mathrm{PGL}(2, q)$. The small projective line over $\mathbb{F}_q$ is embedded into the large projective line over $\mathbb{F}_{q^n}$. A Singer cycle T of H is of order $q+1$. It leaves invariant the small projective line as a set B of $q+1$ points. One of these points is ∞. The stabilizer of B in G is a subgroup G_B containing H. The orbit of B under G is a 3-design since G is 3-homogeneous. This design has

$$b = \lambda \frac{\binom{q^n+1}{3}}{\binom{q+1}{3}}$$

blocks. Also

$$b = |G : G_B| \text{ divides } |G : H| = \frac{\binom{q^n+1}{3}}{\binom{q+1}{3}}.$$

So $\lambda = 1$, $H = G_B$, and the constructed design is a $3\text{-}(q^n+1, q+1, 1)$ design.

For odd n, $q+1$ divides q^n+1 but not q^n-1. So, $|T| = q+1$ does not divide the order $q^n(q^n-1)$ of a point stabilizer in G. Therefore T is generated by an element that has no fixed points on the projective line and thus, lies in a Singer cycle S of G. Since S acts regularly, the subgroup T has all orbits of size $q+1$. One of these orbits is the block B. The orbits of T are transitively permuted by S and so are blocks of $\mathcal{D}$.

The non-identity elements of G have at most two fixed points. From the orders of the point stabilizers in G and H one obtains that elements of H fixing points on the long projective line already fix the same number of points on the small projective line. So, each non-identity element of H has no fixed point outside the small projective line. So, H acts semi-regularly on this set X of $(q^n+1)-(q+1)=q^n-q$ points with $s=\frac{q(q^{n-1}-1)}{q(q^2-1)}$ regular orbits X_i, $i=1,\dots,s$. Together with the orbit B they form a partition $(B,X_1,\dots,X_s)$ of the projective line. They correspond to the double cosets LgH in G, where $L=G_\infty$. Also, the orbit of B under G splits into orbits under L corresponding to double cosets HgL. We have a bijection between the sets of double cosets $L\setminus G/H$ and $H\setminus G/L$ by $Lg^{-1}H\mapsto HgL$. So, there are equally many orbits of both kinds.

The stabilizer L acts transitively on the design derived at ∞. Thus, the orbit of B under L consists of all blocks that contain ∞. If B' is a block not containing ∞ then the stabilizer $L_{B'}$ is trivial. To see this, we use that $H_x=\{id\}$ for each $x\in X$. We have $B^g=B'$ for some $g\in G$ such that $\infty\notin B'=B^g$ and $\infty^{g^{-1}}\notin B$. Thus, $\infty^{g^{-1}}\in X$. Then

$$L_{B'}=G_\infty\cap G_{B'}=G_\infty\cap G_{B^g}=\left(G_\infty^{g^{-1}}\cap G_B\right)^g=(G_{\infty^{g^{-1}}}\cap G_B)^g=\{id\}.$$

Therefore L has orbits of length $|L|=q^n(q^n-1)$ on the set of blocks not containing ∞, that is the residual design.

If X' is an H-orbit on X then X' contains a T-orbit B'. This is a block, since all T-orbits are blocks. So, the regular H-orbit X' splits into B' and the translates of B' under H. The subgroup $H\cap L$ of order $q(q-1)$ already maps B' onto these translates. So, these are sets of size $q+1$ in the same orbit as B'. In particular these are also blocks. There results a partition $B'^{H\cap L}$ of X' into blocks. Choose a T-orbit B_i in each H-orbit X_i on X, $i=1,\dots,s$. Then

$$P=\left(B,B_i^{H\cap L}\;\middle|\;i=1,\dots,s\right)\quad\text{partitions } PG(1,\mathbb{F}_{q^n}).$$

Let $B_i=B^{g_i}$. Then B_i lies in the L-orbit B^{g_iL} that corresponds to the double coset Hg_iL. If $B_i^L=B_j^L$ and $i\neq j$, then $Hg_iL=Hg_jL$ and $Lg_j^{-1}H=Lg_i^{-1}H$. Then $\infty^{g_j^{-1}L}=\infty^{g_i^{-1}L}$. But B_i and B_j were selected from different H-orbits. Thus, the orbits B_i^l, B_j^l are disjoint regular orbits of L on the block set.

Now,

$$\{id\}=L_{B'}<L\cap H<L$$

shows that each $B_i^{L\cap H}$ is a block of imprimitivity of the action of L on the orbit of B_i. By [28, Lemma 2.1],

$$P^L=\left(B,B_i^{H\cap L}\;\middle|\;i=1,\dots,s\right)^L$$

is a resolution of the design.

(ii) Recall that No. 7 in Section 3.3 is obtained by applying Theorem 3.6(ii) to the 3-$(q^n+1,q+1,1)$ design constructed by (i) of this theorem as $\mathcal{D}_2$. The constructed design is resolvable by Theorem 5.1. Generally for $v=2(q^n+1)$ and $\ell=2(q+1)$ we need that $\gcd(2q+1,2q^n+1)=1$ and $\gcd(q+1,2q^n+1)=1$. The latter condition is always true, which shows the assertion. □

There are some observations.

(i) Van Tran found a 3-$(2^{m+1}+2,6,5(2^m-1))$ design, a 3-$(2^n20,8,7(2^{n-2}20-1))$ design, a 3-$(2^n28,8,7(2^{n-2}28-1))$ design for every odd integer $m\geqslant 5$ and every integer $n\geqslant 0$. He does not say anything whether these designs are resolvable. In contrast, the families of Theorem 5.3(i) and (ii) not only include the designs by van Tran, but also are resolvable.

(ii) Resolvable designs which have the same parameters as the designs of Theorem 5.3(iii) can also be obtained by an Alltop-type theorem of van Tran [41, Theorem 2.7].

(iii) Recall a family of Laue which already appears in Section 3.3, that is, a simple 3-$(q+1,(q+1)/2,(q-1)(q-3)/8)$ design. Laue [28, Theorem 3.1] proved that they are all resolvable.

In comparison with his family, the designs of Theorem 5.3(iii) have more general parameters. For example, if q is a prime power with $q \equiv 1 \pmod 4$, by choosing as an embedding design the Paley-type Hadamard matrix of order $2(q+1)$ [36], the designs of Theorem 5.3(iii) have parameters $v = 4q+4, k = 2q+2, \lambda = q(2q-1)$, where q is a prime power with $q \equiv 1 \pmod 4$. It seems to be difficult to construct this family by the group-theoretic way, if $4q+3$ is not a prime power.

(iv) As far as the authors know, the family of Theorem 5.4(i) is the first and only known infinite family of resolvable Steiner t-designs with $t \geqslant 3$ and block size bigger than 4. In Theorem 5.4(ii), when $n = 3$ the condition $\gcd(2q+1, 2q^n+1) = 1$ can be reduced to $q \not\equiv 1 \pmod 3$. When $n = 5$ in addition $q \not\equiv 2 \pmod 5$ is needed.

Finally we close this section by emphasizing that the resolvable 3-designs found in this section could be applied to the basic construction again.

6. Conclusions

The basic construction presented in this paper extends Jungnickel–Vanstone's construction of simple 3-designs with block size four to that of 3-designs with general block sizes. Several known infinite families of simple 3-designs have been unified through our approach and many infinite families whose existence were previously in doubt have been found. The basic construction can also generate designs with various combinatorial properties: For example it yields a design admitting a group of automorphisms when assuming that a master design admits the same group as an automorphism group and an embedding design is a complete design; recall Section 4. Moreover it yields a resolvable design if a master design and an embedding design are both resolvable — we may possibly find more simple 3-designs by repeatedly using the basic construction. Finally, we briefly mention a possibility for further research: There is an approach which generates disjoint copies of a t-design with a small number of blocks on enlarged point sets. It relies on the *Permutation Lemma*; for example see [31,39]. It may well be that our approach can be combined with this approach to get more general results. This will be discussed in a forthcoming paper.

Acknowledgment

We would like to thank Michael Kiermaier for some computational efforts using MAGMA [11].

References

[1] G. Alber, T. Beth, C. Charnes, A. Delgado, M. Grassl, M. Mussinger, Detected-jump-error-correcting quantum codes, quantum error designs, and quantum computation, Phys. Rev. A 68 (2003) 012316.
[2] T. Beth, C. Charnes, M. Grassl, G. Alber, A. Delgado, M. Mussinger, A new class of designs which protect against quantum jumps, Des. Codes Cryptogr. 29 (2003) 51–70.
[3] B.A. Anderson, Finite topologies and Hamiltonian paths, J. Combin. Theory Ser. B 14 (1973) 87–93.
[4] B.A. Anderson, Symmetry groups of some perfect one-factorizations of complete graphs, Discrete Math. 18 (1977) 227–234.
[5] I. Anderson, Combinatorial Designs and Tournaments, Clarendon Press, Oxford, 1997.
[6] L.D. Anderson, Factorizations of graphs, in: C.J. Colbourn, J.H. Dinitz (Eds.), Handbook of Combinatorial Designs, second ed., in: Discrete Math. Appl., Chapman and Hall/CRC Press, Boca Raton, USA, 2007, pp. 740–755.
[7] Z. Baranyai, On the factorization of the complete uniform hypergraph, in: Proc. Erdös Colloquium, Keszthely, 1973, North-Holland, Amsterdam, 1975, pp. 91–108.
[8] T. Beth, D. Jungnickel, Einige einfache fahnenhomogene 3-Blockpläne, Math. Z. 183 (1983) 443–445.
[9] T. Beth, D. Jungnickel, H. Lenz, Design Theory, I, second ed., Encyclopedia Math. Appl., vol. 69, Cambridge Univ. Press, 1999.
[10] J.I. Blanchard, A construction for Steiner 3-designs, J. Combin. Theory Ser. A 71 (1995) 60–66.
[11] W. Bosma, J. Cannon, C. Playoust, The magma algebraic system, I, the user language, J. Symbolic Comput. 24 (1997) 235–265.
[12] P.J. Cameron, Parallelisms of Complete Designs, London Math. Soc. Lecture Note Ser., vol. 23, Cambridge Univ. Press, Cambridge, 1976.
[13] P.J. Cameron, G.R. Omidi, B. Tayfeh-Rezaie, 3-Designs from PGL$(2, q)$, Electron. J. Combin. 13 (2006), Research Paper 50.
[14] R.D. Carmichael, Introduction to the Theory of Groups of Finite Order, Ginn, Boston, 1937.
[15] L.M.H.E. Driessen, t-Designs, $t \geqslant 3$, Tech. Report, Department of Mathematics, Eindhoven University of Technology, 1978.
[16] G.B. Khosrovshahi, R. Laue, in: C.J. Colbourn, J.H. Dinitz (Eds.), Handbook of Combinatorial Designs, second ed., in: Discrete Math. Appl., Chapman and Hall/CRC Press, Boca Raton, USA, 2007, pp. 79–110.

[17] H. Hanani, On some tactical configurations, Canad. J. Math. 15 (1963) 705–722.
[18] A. Hartman, The existence of resolvable Steiner quadruple systems, J. Combin. Theory Ser. A 44 (1987) 182–206.
[19] A. Hartman, The fundamental construction for 3-designs, Discrete Math. 124 (1994) 107–132.
[20] A. Hartman, A. Rosa, Cyclic one-factorization of the complete graph, European J. Combin. 6 (1985) 45–48.
[21] D.R. Hughes, On t-designs and groups, Amer. J. Math. 87 (1965) 761–778.
[22] S. Iwasaki, T. Meixner, A remark on the action of $\mathrm{PGL}(2,q)$ and $\mathrm{PSL}(2,q)$ on the projective line, Hokkaido Math. J. 26 (1997) 203–209.
[23] L. Ji, L. Zhu, Resolvable Steiner quadruple systems for the last 23 orders, SIAM J. Discrete Math. 19 (2005) 420–430.
[24] D. Jungnickel, S.A. Vanstone, Hyperfactorizations of graphs and 5-designs, J. Univ. Kuwait 14 (1987) 213–223.
[25] D. Jungnickel, S.A. Vanstone, On resolvable designs $S_3(3,4,v)$, J. Combin. Theory Ser. A 43 (1986) 334–337.
[26] E. Köhler, k-difference cycles and the construction of cyclic t-designs, in: Geometries and Groups, in: Lecture Notes in Math., vol. 893, Springer-Verlag, Berlin/New York/Heidelberg, 1981, pp. 195–203.
[27] A. Kotzig, Hamilton graphs and Hamilton circuits, in: Theory of Graphs and Its Applications, Proceedings of the Symposium in Smolenice, 1963, Publ. House Czechoslovak Acad. Sci., Prague, 1964, pp. 63–82.
[28] R. Laue, Resolvable t-designs, Des. Codes Cryptogr. 32 (2004) 277–301.
[29] D.C. van Leijenhorst, Orbits on the projective line, J. Combin. Theory Ser. A 31 (1981) 146–154.
[30] J.H. van Lint, R.M. Wilson, A Course in Combinatorics, second ed., Cambridge Univ. Press, Cambridge, 2001.
[31] S.S. Magliveras, T.E. Plambeck, New infinite families of simple 5-designs, J. Combin. Theory Ser. A 44 (1987) 105.
[32] M. Meszka, k-Cycle free one-factorizations of complete graphs, Electron. J. Combin. 16 (2009), Research Paper 3.
[33] I. Miyamoto, A construction of designs on $n+1$ points from multiply homogeneous permutation groups of degree n, J. Combin. Theory Ser. A 117 (2010) 430–439.
[34] H. Mohácsy, D.K. Ray-Chaudhuri, Candelabra systems and designs, J. Statist. Plann. Inference 106 (2002) 419–448.
[35] A. Munemasa, M. Sawa, Simple abelian quadruple systems, J. Combin. Theory Ser. A 114 (2007) 1160–1164.
[36] R.E.A.C. Paley, On orthogonal matrices, J. Math. Phys. 12 (1933) 311–320.
[37] K. Phelps, D.R. Stinson, S.A. Vanstone, The existence of simple $S_3(3,4,v)$, Combinatorial designs—a tribute to Haim Hanani, Discrete Math. 77 (1989) 255–258.
[38] A. Rahilly, Constructing designs using the union method, Australas. J. Combin. 6 (1992) 7–21.
[39] M. Sebille, An extension theorem for t-designs, Discrete Math. 240 (2001) 197–204.
[40] T. van Tran, Construction of 3-designs using parallelism, J. Geom. 67 (2000) 223–235.
[41] T. van Tran, Recursive constructions for 3-designs and resolvable 3-designs, J. Statist. Plann. Inference 95 (2001) 341–358.
[42] R.M. Wilson, An existence theory for pairwise balanced designs, III. Proof of the existence conjectures, J. Combin. Theory Ser. A 18 (1975) 71–79.
[43] E. Witt, Über Steinersche Systeme, Abh. Math. Sem. Univ. Hamburg 12 (1938) 265–275.